BENT FUNCTIONS AND SPREADS

7/23/15

WILLIAM M. KANTOR

Abstract. This note is a response to a request by Claude Carlet for a brief summary of some of what is known about spreads for use in John Dillon's fundamental partial spread construction of bent functions.

This note was not written to be published.

1. Introduction

We assume that readers are familiar with the basic notions regarding bent functions, including partial spreads: a *partial spread* of $\mathbb{F}_2^{2m}$ is a set Σ of m-dimensional subspaces any two of which meet only in 0. The starting point of this note is the following fundamental result constructing bent functions:

Dillon's Theorem [Di, Theorem 5.2.2]. *If Σ is a partial spread of $\mathbb{F}_2^{2m}$ consisting of $2^{m-1}+1$ subspaces, then $\bigcup_{X\in\Sigma} X$ is the support of a bent function on $\mathbb{F}_2^{2m}$.*

There is a variation on this theorem also appearing in [Di, Theorem 5.2.2] that uses 2^{m-1} subspaces, but the preceding version suffices for our purposes.

The present note is intended to provide some information concerning aspects of partial spreads related to finite geometries, in the hope that this will be helpful for bent function researchers. We have tried to be brief, hence not to give details, nor many types of examples, nor examples that are complicated to describe, nor historically complete references. Such a short survey is guaranteed to be biased by this author's tastes.

A partial spread Σ is a *spread* if its union is $\mathbb{F}_2^{2m}$, in which case $|\Sigma| = 2^m+1$. Not all partial spreads are contained in spreads. For example, this occurs for an "orthogonal spread", whose union is the set of zeros of a quadratic bent function [Di] (Dillon used the term "Pall partition" instead of "orthogonal spread"); orthogonal spreads are maximal partial spreads, and there are reasonably large numbers of them (as noted in Question 9 below).

Dillon [Di, pp. 36, 40 and 46] referred to [Os] for the existence of many spreads arising from affine planes. In [Di, Remark 5.4.6] he noted that his theorem applies to each of the $\binom{2^m+1}{2^{m-1}+1}$ choices of $2^{m-1}+1$ members of a spread of $\mathbb{F}_2^{2m}$. Forty years later this observation was revisited in [Ca, Wu, CMP].

Known vs. unknown bent functions. By [LL], there are approximately 2^{106} different bent functions $\mathbb{F}_2^8 \to \mathbb{F}_2$, ignoring the equivalence of such functions (cf. Section 2.2). Moreover, of these fewer than 2^{77} arise from constructions in print, which in turn are dominated by two types of constructions introduced in [Di]: Maiorana-McFarland bent functions and partial spread bent functions. This means that already in a small dimension the known types of constructions are woefully

Key words and phrases. bent function, partial spread, translation plane.

inadequate for describing “most” bent functions. This gap in knowledge increases exponentially as the dimension of the underlying vector space grows.

There are many inequivalent spreads from which to choose partial spreads, but the number of known ones does not help at all to deal with the aforementioned gap.

Other characteristics. Much of this note applies to all characteristics, although various constructions are tied to the parity of the field size. However, our focus is on classical bent functions and hence on vector spaces over the field of order 2.

2. Affine planes

Spreads arise naturally in finite geometry: if $\hat{\Sigma}$ is a spread of $\mathbb{F}_2^{2m}$ then the vectors in $\mathbb{F}_2^{2m}$, together with the translates $X+c$ for $X\in\hat{\Sigma}$ and $c\in\mathbb{F}_2^{2m}$, form the points and lines of an affine plane of order 2^m. Such an affine plane is called a “translation plane”: all translations $v\to v+c,\ c\in\mathbb{F}_2^{2m}$, are collineations (i. e., automorphisms) of this plane. There is a large literature on these planes. This was already noted long ago in [Di, pp. 36, 40 and 46].

Since then the number of papers concerning translation planes has grown enormously. There is now a large, almost encyclopedic book [JJB2] containing a wealth of information about these planes and their associated spreads, together with large related books [JJB1, Jo2]. The crucial point is that are many different constructions known for spreads. Hundreds of different types of constructions are in [JJB2], and there are many more (in the other two books; also see Mathscinet). We will not make any attempt to describe more than a tiny number of types of spreads. We refer to the above books for many far more complicated examples.

2.1. **Prequasifields.** Let $\hat{\Sigma}$ be a spread of $\mathbb{F}_2^{2m}$. *Pick any two members X,Y of $\hat{\Sigma}$. Fix an isomorphism between X and Y.* Then $\mathbb{F}_2^{2m}$ can be viewed as the set of pairs (x,y) with $x,y\in X$, and we can think of $X=[y=0]$ and $Y=[x=0]$ as the x and y “axes”. We emphasize that there were choices made here, there is no “best” choice of the ordered pair $X,Y\in\hat{\Sigma}$. One of the fundamental properties of partial spreads is that the underlying vector space is the direct sum of *any* two of its members (cf. Section 3.1).

Any other member of $\hat{\Sigma}$ can be identified with the set of all pairs (x,Mx) for an invertible linear transformation M of $\mathbb{F}_2^{2m}$. Thus, lines through 0 are just sets of the form $x=0$ and $y=Mx$ (here M is allowed to be O).

The lines through 0 are just the members of $\hat{\Sigma}$, so there are 2^m+1 of them. One of them is X; *label the others bijectively in any way using $\mathbb{F}_2^m$.* Then the lines through 0 look like $x=0$ and $y=M_ax$ for 2^m matrices M_a, $a\in\mathbb{F}_2^m$.

This leads to a *binary operation* on $\mathbb{F}_2^m$:

$$a*x:=M_ax.$$

Since M_a is additive, we have the distributive law $a*(u+v)=a*u+a*v$. The fact that pairs of sets $y=a*x$ meet only in 0 translates to the condition that $a*x=b*x\neq 0\Rightarrow a=b$. Such a system $(\mathbb{F}_2^m,+,*)=(F,+,*)$ is called a *prequasifield.* Note that there are various choices that have been made: $X,Y\in\Sigma$, the isomorphism $X\to Y$, and the labeling of the lines through 0 as $y=M_ax$.

Using the prequasifield $(F,+,*)$, the points of our affine plane are the vectors in F^2, and the lines are $x=c$ and $y=a*x+b$, as in High School.

Quasifields. It is straightforward to relabel in order to have an identity element $1 \in \mathbb{F}_2^m$, so that $1 * a = a = a * 1$ for all $a \in \mathbb{F}_2^m$, in which case our algebraic system is called a *quasifield*. A spread or affine plane described using a prequasifield can always be described using a quasifield isotopic to it (cf. Section 2.2).

Presemifields and semifields. Our prequasifield is a *presemifield* if the other distributive law $(u+v)*a = u*a + v*a$ holds (for all a, u, v); and it is a *semifield* if it is a presemifield with an identity element. Once again, a spread or affine plane described using a presemifield can also be described using a semifield.

Examples: Fields. The *desarguesian affine plane* of order 2^m arises from the spread consisting of the set of 1-spaces of a 2-dimensional vector space over $\mathbb{F}_{2^m}$.

2.2. **Equivalence and automorphism group.**

Bent functions. We view bent functions $f, g\colon \mathbb{F}_2^{2m} \to \mathbb{F}_2$ as *equivalent* if there is an invertible affine transformation M of $\mathbb{F}_2^{2m}$ such that $f(M(v)) = g(v)$ for all $v \in \mathbb{F}_2^m$. Then the notion of *automorphism group* $\mathrm{Aut}(f)$ is clear. The preceding definitions correspond to the standard notions of equivalence and automorphism group of the difference sets associated with the bent functions [Di].

The problem of determining whether bent functions f and g are or are not equivalent is difficult, as is the determination of $\mathrm{Aut}(f)$ (cf. [Be, Ka1, De2]).

Spreads. Similarly, (partial) spreads Σ, Σ' of $\mathbb{F}_2^{2m}$ are *equivalent* if there is an invertible linear transformation (or matrix) $M \in \mathrm{GL}(2m, 2)$ such that $M(\Sigma) = \Sigma'$. The *automorphism group* $\mathrm{Aut}(\Sigma)$ of Σ consists of the elements of $\mathrm{GL}(2m, 2)$ sending Σ to itself.

Prequasifields. Equivalences of prequasifields are called *isotopisms*: prequasifields $(F, +, *)$ and $(F', +, \circ)$ using binary vector spaces F and F' are *isotopic* if there is a triple (α, β, γ) of bijections $F \to F'$ such that β and γ are additive, $\alpha(0) = 0$, and $\gamma(u * v) = \alpha(u) \circ \beta(v)$ for all $u, v \in F$. See [JJB2, Sec. 5.4] for a discussion of this notion, in particular for the following results and many more: isotopic prequasifields determine equivalent spreads, **but the converse is false**.

In order to understand this remark, start with spreads $\hat{\Sigma}$ in F^2 and $\hat{\Sigma}'$ in F''^2 for isomorphic (binary) vector spaces F and F'. Choose ordered pairs $X, Y \in \hat{\Sigma}$ and $X', Y' \in \hat{\Sigma}'$ in order to obtain prequasifields $(F, +, *)$ and $(F', +, \circ)$. Then *there is an additive isomorphism $F^2 \to F'^2$ sending $X \to X'$ and $Y \to Y'$ if and only if the corresponding prequasifields $(F, +, *)$ and $(F', +, \circ)$ are isotopic*; this is a straightforward calculation using the definitions (cf. [JJB2, Sec. 5.4]). We will see what this means more precisely in Section 3.1. For now we note that a given spread $\hat{\Sigma}$ need not have many automorphisms, hence there may be many essentially different ways to choose an ordered pair of its members, producing many non-isotopic prequasifields.

Of course, the most familiar example occurs for a desarguesian affine plane, where the automorphism group of the spread is 2-transitive on the spread and hence all pairs X, Y are "indistinguishable".

2.3. **Bent functions from prequasifields.** Once again this was foreseen in [Di] as an application of Dillon's Theorem. If $(\mathbb{F}_2^m, +, *)$ is a prequasifield let $g\colon \mathbb{F}_2^m \to \mathbb{F}_2$ be any balanced function[1] such that $g(0) = 0$, and define $f(x, y) := g(y/x)$ where $(y/x) * x = x$, with the convention that $g(y/0) = 0$. *Then f is a bent function.*

[1] A *balanced function* takes each value equally often.

Once again we note that there was a choice made of members $x = 0$ and $y = 0$ of the spread. Different choices usually give nonisotopic prequasifields, and presumably will often produce inequivalent bent functions.

3. Examples

Before giving some examples we need to emphasize that *most of the known types of spreads are not described using prequasifields.* In other words, the description used in Section 2.3 is very special in view of published examples. See Section 3.7 for some examples. By contrast, semifield spreads are always described using more or less explicit presemifields, but there are far fewer of these known than for more general prequasifields.

3.1. **Changing X and Y.**

Before giving explicit examples we indicate the change of "coordinates" in the choices made in Section 2.1 and discussed in Section 2.2.

Start with a prequasifield $(F, +, *)$, and consider $V = F^2$, so V is naturally $X \oplus Y$ for $X = [y = 0]$ and $Y = [x = 0]$, the x- and y-"axes". Fix distinct nonzero $c, d \in F$, and let $X' = [y = c * x]$ and $Y' = [y = d * x]$. (This considers most but not all possible choices of ordered pairs X', Y' of members of our spread.) We will replace the decomposition $F^2 = X \oplus Y$ by the direct sum decomposition of F^2 using X' and Y' in order to obtain a new prequasifield operation.

Each point of the line $y = a * x$ looks like $(x, a * x) = (u, c * u) + (v, d * v)$ for unique $(u, c * u) \in X'$, $(v, d * v) \in Y'$. Then u is a function of a and x, say $u = G(a, x)$, that is additive in x and is determined as the unique solution to the equation $a * x = c * G(a, x) + d * [G(a, x) + x]$. (Here, $v = G(a, x) + x$.)

Recall that we obtain a prequasifield using additive isomorphisms such as $(x, 0) \to x$ and $(0, y) \to y$ (cf. Section 2.1): $(x, a * x) = (x, 0) + (0, y)$ where the "X"-coordinate is x and the "Y"-coordinate is $y = a * x$. There are additive bijections $X' \to F$ via $(u, c*u) \to u$ and $Y' \to F$ via $(v, d*v) \to v$ (recall that c and d do not vary here). In the equation $(x, a*x) = (u, c*u)+(v, d*v)$ we have "X'"-coordinate u and the "Y'"-coordinate v, so write $v = a \circ u$. Then the equations

$$a \circ G(a, x) = G(a, x) + x, \qquad a * x + d * x = c * G(a, x) + d * G(a, x)$$

implicitly define the new prequasifield $(F, +, \circ)$.[2] In order to calculate $a \circ u$ we would have to solve the equation $u = G(a, x)$ for x in terms of a and u. *We leave it to the reader to try to calculate the operation $\circ$ explicitly in the examples below.* The equations to be solved are often disgusting.

For most choices of $*, c, d$ the new prequasifield is not isotopic to the original one: in Section 2.2 we noted that isotopism amounts to the existence of an automorphism of the spread sending $X \to X'$ and $Y \to Y'$. So the above process yields many "new" prequasifields *producing the same spread and hence the same partial spreads* in Dillon's Theorem. If $*$ is a presemifield operation but the spread is not desarguesian, then $\circ$ will not be isotopic to a presemifield.

3.2. **Examples: André prequasifields** [An].

Start with a finite field F, a proper subfield K with associated norm map $N : F \to K$, and an arbitrary map α from $K^* = K\backslash\{0\}$ to the Galois group $\mathrm{Gal}(F/K)$. Then $0 * x = 0$ and

$$a * x := a x^{\alpha(N(a))}, \ a \in F^*, \ x \in F,$$

[2] In place of "$a \circ$" on the left we could have used "$\alpha(a) \circ$" for any permutation α of X fixing 0, obtaining an isotopic prequasifield. For the same reason we do not need to use a copy F' of F.

defines a prequasifield. (Proof: $ax^{\alpha(N(a))} = bx^{\alpha(N(b))} \neq 0 \Rightarrow N(a)N(x) = N(ax^{\alpha(a)}) = N(b)N(x) \neq 0 \Rightarrow ax^{\alpha(N(a))} = bx^{\alpha(N(a))} \Rightarrow a = b$.)

These easily described prequasifields were among the first to be studied. When $[F\colon K] = 2$ the resulting spreads appeared in a very different and independently obtained description in [Br]; and those spreads and variations [BEP] provide asymptotically "most" (up to isotopism, cf. Section 2.2) of the known examples of prequasifields of size $|F|$, due to the large number of choices for the map $\alpha\colon K^* \to \mathrm{Gal}(F/K) \cong \mathbb{Z}_2$.

Many variations on André's construction appear in [JJB2].

3.3. **Examples: Knuth's "binary semifields"** [Kn2]**.** Let K be a proper subfield of $F = \mathbb{F}_{2^m}$ with $[F\colon K]$ odd and associated trace map $T\colon F \to K$. Then

$$x * y := xy + (xT(y) + yT(x))^2,\ \ x, y \in F,$$

defines a *commutative* presemifield operation on F. (Proof: $0 \neq xy = x^2T(y)^2 + y^2T(x)^2 \Rightarrow (y/x)^2T(x)^2 + (y/x) + T(y)^2 = 0 \Rightarrow [\textit{since } [F\colon K] \textit{ is odd}]\ \ y/x = a \in K \Rightarrow a^2T(x)^2 + a + (aT(x))^2 = 0 \Rightarrow a = 0$, whereas $y \neq 0$.) If $m > 3$ then this produces a spread Σ whose automorphism group fixes $x = 0$ and is transitive on the remaining members of Σ.

There is a generalization of these examples [Ka3] obtained using orthogonal geometries, arbitrarily long chains of fields instead of $F \supset K$, and a more complicated formula for $*$ than the above one. These and related presemifields [KaW2, Ka3] account for most of the *known* presemifields of size 2^m, in the sense that (up to isotopism) their number is not bounded above by any polynomial in 2^m, whereas there are $O(m2^{2m})$ other known presemifields of size 2^m (up to isotopism).

3.4. **Examples: More semifields due to Knuth** [Kn1]**.** Let $f, g \in F = \mathbb{F}_{2^m}$ and $1 \neq \sigma \in \mathrm{Aut}(F)$ be such that the polynomial $t^{\sigma+1} + gt + f$ has no root in F. Then it is straightforward to check that each of the following rules for $(a, b) * (c, d)$ produces a noncommutative semifield $(F^2, +, *)$:

(1) $(ac + fb^\sigma d^{\sigma^{-2}}, bc + a^\sigma d + gb^\sigma d^{\sigma^{-1}})$
(2) $(ac + fb^\sigma d, bc + a^\sigma d + gb^\sigma d)$
(3) $(ac + fb^{\sigma^{-1}} d^{\sigma^{-2}}, bc + a^\sigma d + gbd^{\sigma^{-1}})$
(4) $(ac + fb^{\sigma^{-1}} d, bc + a^\sigma d + gbd)$.

In each case the "dual plane" arises from the semifield operation $x \circ y := y * x$ [JJB2, p. 43].

3.5. **Examples: A recursive construction** [HMO]**.** Since 2×2 matrices are easier to deal with than larger matrices, early prequasifield constructions used K^2, $K = \mathbb{F}_q$, with an operation of the form

$$(a, b) * (x, y) := (a, b) \begin{pmatrix} x & y \\ g(x, y) & h(x, y) \end{pmatrix}$$

for all $a, b, x, y \in K$. (For example, consider $\mathbb{F}_{q^2}$.) We leave to the reader the condition on the functions g, h in order to obtain a prequasifield.

Let $F = \mathbb{F}_{q^2} \supset K$ and $r \in F \backslash K$ with $r^2 + r \in K$. For $v = x + ry \in F$ $(x, y \in K)$ let $f(v) := h(x, y) + g(x, y) + h(x, y)r$. Then it is straightforward to check that

$$(\alpha, \beta) \circ (u, v) := (\alpha, \beta) \begin{pmatrix} u & v \\ f(v) & u^q \end{pmatrix}$$

defines a prequasifield on F^2. This construction produces both presemifield spreads and spreads not obtainable from presemifields [Jo1], and can be repeated using fields of order q^{2^k} containing F, where $k = 2, 3, \ldots$.

3.6. **Examples: Jha-Johnson presemifields** [JJ]**.** For a d–dimensional vector space V over a finite field K, let $T\colon V \to V$ be an irreducible semilinear transformation (that is, T is additive, satisfies $T(av) = \sigma(a)T(v)$ for some $\sigma \in \mathrm{Aut}(K)$ and all $a \in K, v \in V$, and *leaves invariant no proper K-subspace of V*). Then $S := \sum_0^{d-1} KT^i$ is a vector space of $|V|$ endomorphisms of the binary vector space V; choose any additive isomorphism $h\colon V \to S$. Then $u * v := h(u)\big(v\big), u, v \in V$, defines a presemifield operation on V. (Proof. If $(\sum_0^{d-1} a_iT^i)(v) = 0 \neq v$ and at least one $a_i \in K^*$, let $1 \le r \le d-1$ with $0 \neq a_rT^r(v) = -(\sum_0^{r-1} a_iT^i)(v)$. Since all powers of T are semilinear, $T(KT^{r-1}(v)) = Ka_rT^r(v) = K(\sum_0^{r-1} a_iT^i)(v) \subseteq \sum_0^{r-1} KT^i(v)$, so the latter is a proper T-invariant subspace, which is a contradiction.)

This construction is based on a standard description of a field of order $|V|$ that occurs when $\sigma = 1$. There seems to be a lot of flexibility in this description, but in fact fewer than $|V|\log_2|V|$ inequivalent spreads are obtained [KL]. All possible T are described in [De3].

3.7. **Spreads constructed without the use of prequasifields.** We have already observed that most known constructions behave in this manner [JJB2]. We mention a few instances.

1. Spreads of $(\mathbb{F}_{q^3})^2$ on which $\mathrm{GL}(2,q)$ acts with orbits of size $q+1$ and q^3-q [JJ]: in Example 3.6 let $V = F$ and $F = \mathbb{F}_{q^3} \supset K = \mathbb{F}_q$, with T not K-linear (i. e., $\sigma \neq 1$). The desired spread consists of the following q^3+1 additive subgroups of F^2: $x = 0$, $y = ax$ with $a \in K$, and $q^3 - q$ subgroups $\{(x, T(x))\big(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\big) \,|\, x \in F\}$ for $a, b, c, d \in K$ with $\det\big(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\big) \neq 0$. (Proof. $(v, T(v)) = (u, T(u))\big(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\big) \neq 0 \Rightarrow T(ua + T(u)c) = ub + T(u)d \Rightarrow TT(u)\sigma(c) + T(u)(\sigma(a) - d) - ub = 0$. If $\sigma(c) \neq 0$ then $T^2(u) \in Ku + KT(u)$, whereas the K-space $Ku + KT(u) \neq T(Ku + KT(u))$ (cf. Example 3.6). Similarly, $\big(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\big) = \big(\begin{smallmatrix} a & 0 \\ 0 & \sigma(a) \end{smallmatrix}\big)$, so that $\{(x, T(x))\big(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\big) \,|\, x \in F\} = \{(x, T(x)) \,|\, x \in F\}$. Thus, the different subgroups $\{(x, T(x))\big(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\big) \,|\, x \in F\}$ pairwise meet in 0, and there are $|\mathrm{GL}(2,q)|/(q-1) = q^3 - q$ of them.)

The nonlinearity of T implies that the spread is not desarguesian.

2. Spreads for which there is a cyclic group of automorphisms transitive on the spread [KaW1], described using the behavior of this cyclic group rather than a prequasifield. We give an example.

Start with $F = \mathbb{F}_{q^{2m}} \supset L = \mathbb{F}_{q^m}$ with $m > 1$ odd, the trace map $T\colon L \to \mathbb{F}_q$, $r \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$, and $s \in F^*$ of order q^m+1. If $h(x) := T(x) + rx$, then $\{s^ih(L) \mid 0 \le i \le q^m\}$ is a spread. (Proof: Let "bar"$\in \mathrm{Aut}(F)$ have order 2. If $s^i[T(x)+rx] = T(y)+ry \neq 0$ with $s^i \neq 1$ then $x + y \neq 0$. Multiply by the bar-image: $T(x)^2 + (r+\bar r)xT(x) + r\bar r x^2 = T(y)^2 + (r+\bar r)yT(y) + r\bar r y^2 \Rightarrow$ [*applying T*] $T(x)^2 + (r+\bar r)T(x)T(x) + r\bar r T(x^2) = T(y)^2 + (r+\bar r)T(y)T(y) + r\bar r T(y^2) \Rightarrow (1+r)(1+\bar r)(T(x)^2 + T(y)^2) = 0 \Rightarrow (r+\bar r)(x+y)T(x) + r\bar r(x+y)^2 = 0 \Rightarrow r\bar r(x+y) = (r+\bar r)T(x) \in L \Rightarrow$ [*applying T*] $r\bar r(x+y) = T(r\bar r(x+y)) = r\bar r(T(x) + T(y)) = 0$, whereas $x + y \neq 0$.)

This spread is not desarguesian if $|F| > 8$. A much more complicated version of this construction replaces the pair $L \supset \mathbb{F}_q$ by an arbitrarily long chain of fields [KaW1]. These examples, and those alluded to in the second paragraph of Section 3.3, did not arise due to any kind of experimentation. They were forced by considerations of high-dimensional orthogonal geometries.

3. Spreads corresponding to the Lüneburg-Tits planes [Lü]. The Suzuki simple group $\mathrm{Sz}(q)$ acts 2-transitively on such a spread, just like $\mathrm{SL}(2, q)$ acts 2-transitively on a desarguesian spread. See [Lü, (13.1)] for a description in terms of coordinates, using a nonabelian group of order q^2.

4. Spreads whose full automorphism group has order 1 ([Ka2] constructs more than 2^m pairwise inequivalent spreads of this sort in $(\mathbb{F}_2^m)^2$ for composite m relatively prime to 6). There is no reasonable way to describe these spreads in terms of a choice of members X and Y of the spread. It is dubious that such a spread could be described in any meaningful way via a prequasifield.

4. Which bent functions are especially "useful"?

In this section we consider questions about "useful" bent functions, as well as about properties of bent functions. The word "useful" is intentionally vague: it refers to known or future uses either in mathematics or in applications. As with the rest of this note, the questions are a bit biased. It is hoped that none of the answers are too obvious.

Question 1. Which should come first: obtain a long list of "explicit" bent functions and then try to decide which are useful? Or first decide on criteria for usefulness of bent functions and then try to find many of them?

The first of these seems especially hard: given a list of dozens or even hundreds of functions, how can one "see" anything useful, how can one even focus on so many functions? Nevertheless, cataloguing a large number of bent functions appears to be viewed in part as "data collection" for possible eventual use.

Question 2. Are univariate (or bivariate) bent functions especially useful? If so, would this make many partial spread and Maiorana-McFarland [Di] bent functions less interesting?

Question 3. Are normal bent functions especially useful? Are non-normal bent functions especially useful? Are there large numbers of non-normal bent functions (cf. [CDDL])? Here a bent function on $\mathbb{F}_2^{2m}$ is *normal* if it is constant on some m-dimensional affine subspace.

Question 4. Is every finite group isomorphic to $\mathrm{Aut}(f)$ for some bent function f? Or even for a bent function f obtained in Dillon's Theorem?

Certainly every finite group is isomorphic to a subgroup of some $\mathrm{Aut}(f)$, namely when f is a quadratic form. Motivating this question are the many theorems of the following sort: every finite group is isomorphic to $\mathrm{Aut}(X)$ for some given type of combinatorial object X, such as a graph, a symmetric design, etc.

Question 5. Are bent functions f such that $\mathrm{Aut}(f) = 1$ especially useful? Are they more "random" than the bent functions appearing in familiar constructions?

Presumably "most" bent functions behave this way, but very few appear to be known and only in $\mathbb{F}_2^8$: one in [Be, p. 91], and 166 of partial spread type in [De2, p. 1117]. Many more such functions are needed! Compare Question 13.

Question 6. Are bent functions especially useful if they arise from Dillon's Theorem via a partial spread Σ for which $\mathrm{Aut}(\Sigma)$ is transitive on Σ?

The only known partial spreads of this type appear to be those arising from quadratic bent functions. There are many variations on this type of question, such as:

Question 7. Are bent functions f for which $\mathrm{Aut}(f)$ is transitive on both $f^{-1}(0)$ and $f^{-1}(1)$ especially useful? All such f have been determined [De1].

More generally: are bent functions f for which $\mathrm{Aut}(f)$ is transitive on $f^{-1}(0)$ especially useful? Determining all such bent functions may be difficult.

Question 8. Are bent functions especially useful if they arise from Dillon's Theorem via a partial spread Σ for which $\mathrm{Aut}(\Sigma)$ fixes one member of Σ and is transitive on the remaining members (cf. [KaW2, Lemma 2.21])?

Question 9. Are bent functions on $\mathbb{F}_2^{2m}$ especially useful if they arise from Dillon's Theorem via a partial spread Σ for which $\mathrm{Aut}(\Sigma) = 1$?

It is not hard to construct reasonably large numbers of such partial spreads (exponential in m) – in fact, partial spreads not properly contained in other partial spreads – by modifying suitable orthogonal spreads. (Of course, the resulting bent functions are not quadratic.)

Finally, we turn to a partial spread Σ as in Dillon's Theorem that is contained in a spread $\hat{\Sigma}$. First, it may be worth noting that Σ can be contained in a large number of spreads $\hat{\Sigma}$ (even: inequivalent spreads; even: Σ can be contained in both desarguesian and nondesarguesian spreads). This occurs in Example 3.2 and variations [BEP].

Question 10. Are there any relationships or differences among the various bent functions obtained from subsets of a spread $\hat{\Sigma}$, especially if the balanced function g in Section 2.3 is restricted somehow? For example, if g is chosen to be random, do the resulting bent functions differ in some significant manner? Alternatively, what if g is a linear functional?

Question 11. If $\hat{\Sigma}$ contains partial spreads Σ_i, $i = 1, 2$, with associated bent functions f_i in Dillon's Theorem, are there circumstances that relate equivalence of the functions and equivalence of the partial spreads? Can the balanced function g in Section 2.3 be carefully chosen to produce such an equivalence of equivalences?

It is probably worth mentioning that, for bent functions f_i determined by partial spreads Σ_i, $i = 1, 2$, if Σ_1 and Σ_2 are equivalent then so are f_1 and f_2. However, *the converse if false*; for example, there are many orthogonal spreads that are partial spreads producing the *same* quadratic bent function [KaW1, KaW2]. (Presumably containment in a spread $\hat{\Sigma}$ does not prevent the existence of examples.)

Question 12. Is there any relationship between the automorphism group of $\hat{\Sigma}$ and the automorphism groups of any of the associated partial spread bent functions (even for carefully chosen balanced functions g in Section 2.3)?

Question 13. Is a bent function on $\mathbb{F}_2^{2m}$ especially useful if it arises from a partial spread Σ for which $\mathrm{Aut}(\hat{\Sigma}) = 1$?

This means that there are no nontrivial scalar transformations available (over some proper extension of $\mathbb{F}_2$, as occur, for example, in the desarguesian case using $(x, y) \to (ax, ay)$, cf. Section 2.1). Nevertheless, the number of such spreads $\hat{\Sigma}$ is exponential in m (cf. Example 3.7.4).

Given such a spread, it should be possible to prove that $\mathrm{Aut}(f) = 1$ for many of the associated bent functions f; or alternatively, for carefully chosen balanced functions g in Section 2.3 (cf. Question 5).

Question 14. Is a bent function arising from Σ especially useful if $\mathrm{Aut}(\hat{\Sigma})$ is transitive on $\hat{\Sigma}$?

This is the primary source of partial spread bent functions provided by Dillon using desarguesian spreads (cf. Section 2.1). However, there are many other spreads with this property (cf. Example 3.7.2).

Question 15. Is a bent function arising from Σ especially useful if $\hat{\Sigma}$ comes from a *presemifield* (cf. Section 2.1)? Or even to a *commutative* presemifield (cf. [CMP])?

The number of such spreads $\hat{\Sigma}$ is not bounded above by any polynomial in 2^m [KaW2, Ka3].

Question 16. Is a bent function arising from Σ especially useful if $\hat{\Sigma}$ comes from a prequasifield having *associative* multiplication but not isotopic to a field? The number of such prequasifields of size 2^m is at most m and hence is rather limited [Za].

Question 17. Is a bent function arising from Σ especially useful if $\hat{\Sigma}$ comes from a prequasifield obtained using 2×2 matrices as in Example 3.5?

Question 18. When $\hat{\Sigma}$ arises from a presemifield, there is a dual plane also coordinatized by a presemfield, as at the end of Section 3.4. (Nothing new is obtained in the commutative case.) Are there relationships between bent functions produced by this pair of dual planes (cf. [CMP])?

Question 19. Some (partial) spreads on $\mathbb{F}_2^{2m}$ are *symplectic*: there is a nondegenerate alternating bilinear form $(\ ,\ )$ on $\mathbb{F}_2^{2m}$ such that $(X, X) = 0$ for all X in the (partial) spread. Desarguesian spreads are examples, as are the spreads in Sections 3.7.2–3.7.4 and all orthogonal spreads. Subsets of a symplectic spread are symplectic. Before 2013 all partial spreads used to construct bent functions were symplectic.

Do bent functions arising from symplectic partial spreads have useful special properties?

The number of such spreads $\hat{\Sigma}$ is not bounded above by any polynomial in 2^m [KaW2].

Question 20. Symplectic partial spreads may be especially suitable for use with bent functions since all linear functionals on $\mathbb{F}_2^{2m}$ arise as $v \to (v, c)$, $c \in \mathbb{F}_2^{2m}$. Is there any advantage to the study of bent functions using an alternating bilinear form in place of the more familiar dot product?

5. Summary

We have probably asked too many questions concerning bent functions. If 20 questions seem too many to focus on, how can 20 formulas for bent functions be sufficiently helpful? Or 200 formulas for bent functions?

It is hoped that this note will stimulate discussions concerning properties of bent functions.

References

[An] J. André, Über nicht-Desarguessche Ebenen mit transitiver Translationsgruppe. Math. Z. 60 (1954) 156–186.

[BEP] R. D. Baker, G. L. Ebert and T. Penttila, Hyperbolic fibrations and q-clans. Des. Codes Cryptogr. 34 (2005) 295–305.

[Be] T. D. Bending, Bent functions, SDP designs and their automorphism groups. Ph.D. thesis, Queen Mary and Westfield College 1993.

[Br] R. H. Bruck, Construction problems of finite projective planes, pp. 426–514 in: Combinatorial Mathematics and its Applications (R. C. Bose and T. A. Dowling, eds.), U. N. Carolina Press, Chapel Hill 1969.

[Ca] C. Carlet, More PS and H-like bent functions (preprint).

[CDDL] A. Canteaut, M. Daum, H. Dobbertin and G. Leander, Finding nonnormal bent functions. Discrete Appl. Math. 154 (2006) 202–218.

[CMP] A. Çeşmelioğlu, W. Meidl and A. Pott, Bent functions, spreads, and o-polynomials. SIAM J. Discrete Math. 29 (2015) 854–867.

[De1] U. Dempwolff, Primitive rank 3 groups on symmetric designs. Des. Codes Cryptog. 22 (2001) 191–207.

[De2] U. Dempwolff, Automorphisms and equivalence of bent functions and of difference sets in elementary abelian 2-groups. Comm. Algebra 34 (2006) 1077–1131.

[De3] U. Dempwolff, Autotopism groups of cyclic semifield planes. J. Algebraic Combin. 34 (2011) 641–669.

[Di] J. F. Dillon, Elementary Hadamard difference sets. Ph.D. thesis, U. of Maryland 1974.

[HMO] Y. Hiramine, M. Matsumoto and T. Oyama, On some extension of 1-spread sets. Osaka Math. J. 24 (1987) 123-137.

[JJ] V. Jha and N. L. Johnson, Translation planes of large dimension admitting nonsolvable groups. J. Geom. 45 (1992) 87–104.

[Jo1] N. L. Johnson, Sequences of derivable translation planes. Osaka J. Math. 25 (1988) 519–530.

[Jo2] N. L. Johnson, Combinatorics of spreads and parallelisms. CRC Press, Boca Raton 2010.

[JJB1] N. L.Johnson, V. Jha andM. Biliotti, Foundations of translation planes. Dekker, NY 2001.

[JJB2] N. L. Johnson, V. Jha and M. Biliotti, Handbook of finite translation planes. Chapman & Hall/CRC, Boca Raton 2007.

[Ka1] W. M. Kantor, Exponential numbers of two-weight codes, difference sets and symmetric designs. Discrete Math. 46 (1983) 95-98.

[Ka2] W. M. Kantor, Projective planes of order q whose collineation groups have order q^2. J. Alg. Comb. 3 (1994) 405–425.

[Ka3] W. M. Kantor, Commutative semifields and symplectic spreads. J. Algebra 270 (2003) 96–114.

[KL] W. M. Kantor and R. A. Liebler, Semifields arising from irreducible semilinear transformations. J. Aust. Math. Soc. 85 (2008) 333–339.

[KaW1] W. M. Kantor and M. E. Williams, New flag-transitive affine planes of even order. JCT(A) 74 (1996) 1–13.

[KaW2] W. M. Kantor and M. E. Williams, Symplectic semifield planes and $\mathbb{Z}_4$-linear codes. TAMS 356 (2004) 895–938.

[Kn1] D. E. Knuth, Finite semifields and projective planes. J. Algebra 2 (1965) 182–217.

[Kn2] D. E. Knuth, A class of projective planes. TAMS 115 (1965) 541–549.

[LL] P. Langevin and G. Leander, Counting all bent functions in dimension eight 99270589265934370305785861242880. Des. Codes Cryptogr. 59 (2011) 193–205.

[Lü] H. Lüneburg, Die Suzukigruppen und ihre Geometrien. Springer, Berlin 1965

[Os] T. G. Ostrom, Finite translation planes. LNM 158, Springer, Berlin-Heidelberg-NY 1970.

[Wu] B. Wu, PS bent functions constructed from finite pre-quasifield spreads, arXiv:1308.3355v1.

[Za] H. Zassenhaus, Über endliche Fastkörper. Abh. Math. Sem. Hamb. 11 (1935) 187–220.

E-mail address: `kantor@uoregon.edu`